

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently amended) A computer-implemented method for training a database intrusion detection system in real time, said method comprising the steps of:
observing, in real time, commands that are accessing the database during a training phase;~~and~~
grouping the commands into categories;
performing a statistical analysis of the categories;
deriving from said commands, in real time, a set of acceptable commands; ~~and~~
ending the training phase responsive to the statistical analysis.
2. (Canceled)
3. (Currently amended) The method of claim-~~2~~ 1 wherein the commands are SQL commands.
4. (Currently amended) The method of claim 1 wherein at least one observed command is selected from the group of commands ~~comprising~~ consisting of a query, an add, a delete, and a modify.
5. (Canceled)
6. (Currently amended) The method of claim-~~5~~ 1 wherein the categories comprise at least one category selected from the group of categories ~~comprising~~ consisting of:
canonicalized commands;
dates and times at which commands access the computer code;
logins of users that issue commands;
identities of users that issue commands;
departments of users that issue commands;
applications that issue commands;

IP addresses of issuing users;
frequency of issuing commands by users;
identities of users accessing a given field within the database;
times of day that a given user accesses a given field within the database;
fields accessed by commands;
combinations of fields accessed by commands;
tables within the database accessed by commands; and
combinations of tables within the database accessed by commands.

7. (Currently amended) The method of claim-~~5~~ 1 wherein:
the categories comprise canonicalized commands; and
each category is a command stripped of literal field data.

8. (Original) The method of claim 1 wherein the observing step comprises at least one of:
real-time auditing; and
in-line interception.

9. (Previously presented) The method of claim 8 wherein the observing step comprises real-time auditing; and at least one of the following is used to extract the commands for observation:
an API that accesses the database;
code injection;
patching;
direct database integration.

10. (Currently amended) The method of claim 8 wherein the observing step comprises in-line interception; and at least one of the following is interposed between senders of the commands and the database:
a proxy;
a firewall;
a sniffer;

11. (Currently amended) The method of claim 1 wherein:
during the deriving step, a suspicious activity is tracked; and
subsequent to the deriving step, the suspicious activity is reported to a system administrator.

12. (Canceled)

13. (Currently amended) The method of claim 1 further comprising, subsequent to the deriving step, an operational step phase in which commands that are accessing the database are compared against the set of acceptable commands.

14. (Currently amended) The method of claim 13 wherein a command that is accessing the database during the operational step phase that does not match a command in the set of acceptable commands is flagged as suspicious.

15. (Previously presented) The method of claim 14 wherein, when a command is flagged as suspicious, at least one of the following is performed:
an alert is sent to a system administrator;
the command is not allowed to access the database;
the command is allowed to access the database, but the access is limited;
the command is augmented;
a sender of the command is investigated.

16. (Currently amended) A computer-readable medium containing computer program instructions for training a database intrusion detection system in real time, said computer program instructions performing the steps of:

observing, in real time, commands that are accessing the database during a training phase; ~~and~~
grouping the commands into categories;
performing a statistical analysis of the categories;
deriving from said commands, in real time, a set of acceptable commands; ~~and~~
ending the training phase responsive to the statistical analysis.

17. (Canceled)

18. (Currently amended) The computer-readable medium of claim ~~17~~ 16 wherein:
the categories comprise canonicalized commands; and
each category is a command stripped of literal field data.

19. (Currently amended) The computer-readable medium of claim 16 further comprising, subsequent to the deriving step, an operational step phase in which commands that are accessing the database are compared against the set of acceptable commands.

20. (Currently amended) ~~Apparatus~~ A computer-readable storage medium storing computer-executable program code for training a database intrusion detection system in real time, ~~said apparatus~~ the computer-executable code comprising:

a training module adapted for observing, in real time, commands that are
accessing the database during a training phase, establishing categories responsive to the observed commands, grouping the commands into the categories, performing a statistical analysis of the categories to determine whether a predetermined frequency threshold for establishing the categories has been exceeded, and for deriving from ~~said the~~ the commands, in real time, a set of acceptable commands; and ending the training phase responsive to a determination that the predetermined frequency threshold has been exceeded; and

coupled to the set of acceptable commands, a comparison module for comparing the commands that access the database during an operational phase with the commands in the set of acceptable commands.

21. (Previously presented) A computer-readable medium containing computer program instructions for providing a database intrusion detection system, said computer program instructions performing steps comprising:

observing commands that are accessing a database during a training phase, the commands comprising literal field data;

stripping the commands of literal field data to produce commands in canonical forms;
grouping the commands responsive to the commands' canonical forms;
generating a set of acceptable commands responsive to the grouped commands;
comparing commands that access the database during an operation phase with commands in the set of acceptable commands; and
flagging as suspicious a command that accesses the database during an operation phase responsive to a determination that the command is not in the set of acceptable commands.

22. (New) The method of claim 1, further comprising the step of establishing new categories responsive to the observed commands, and wherein:

the statistical analysis determines whether a predetermined frequency threshold for establishing the new categories has been exceeded; and
the training phase ends responsive to a determination that the predetermined frequency threshold has been exceeded.

23. (New) The method of claim 1, further comprising the step of establishing new categories responsive to the observed commands, and wherein:

the statistical analysis determines whether a predetermined threshold number of the new categories has been exceeded; and
the training phase ends responsive to a determination that the predetermined threshold number has been exceeded.

24. (New) The method of claim 1, further comprising:

determining whether a predetermined period of time for the training phase has elapsed; and
ending the training phase responsive to a determination that the predetermined period of time has elapsed.